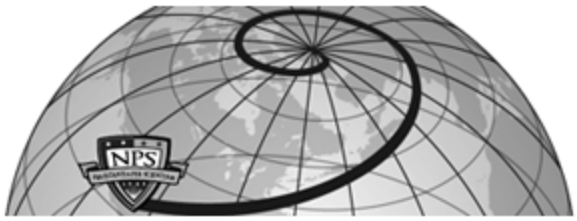

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EFFECTIVE ELECTRONIC SECURITY: PROCESS FOR THE DEVELOPMENT AND VALIDATION FROM REQUIREMENTS TO TESTING

by

James A. Prokop

June 2013

Thesis Advisor: Lauren Fernandez
Second Reader: Nadav Morag

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE EFFECTIVE ELECTRONIC SECURITY: PROCESS FOR THE DEVELOPMENT AND VALIDATION FROM REQUIREMENTS TO TESTING			**5. FUNDING NUMBERS**
6. AUTHOR(S) James A. Prokop			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

An electronic physical security system will often fail to meet user expectations or even basic needs. The inability to easily determine if the system is effective is a key symptom of this failure. This paper explored the process for development, implementation and testing of an electronic security solution. This was accomplished by asking "What is a simple and repeatable systems engineering process that promotes an effective electronic physical security system?" An effective solution was not identified within the literature review process. The Requirements, Alternative, Design, Implementation, Testing and Commissioning (RADITC) process was developed as an alternative solution for the development and validation, from requirements to testing, of an effective physical security solution. The new process is based on two existing processes. The first is a commercial best practice as articulated by Thomas J Whittle. This provides a good foundation of activities. A second more complex life cycle management process used by the Department of Defense (DoD) and Department of Homeland Security (DHS) provided steps and concepts that are missing from the commercial best practices in use today. This resulted in an effective, easy to use and repeatable process.

14. SUBJECT TERMS Electronic Physical Security System, Development Process, Electronic Security Solution			**15. NUMBER OF PAGES** 65
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EFFECTIVE ELECTRONIC SECURITY: PROCESS FOR THE DEVELOPMENT AND VALIDATION FROM REQUIREMENTS TO TESTING

James A. Prokop
Program Manager, Department of Homeland Security
M.S., Capella University, 2010

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2013**

Author: James A. Prokop

Approved by: Lauren Fernandez, DSc
Thesis Advisor

Nadav Morag, PhD
Second Reader

Harold A Trinkunas, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

An electronic physical security system will often fail to meet user expectations or even basic needs. The inability to easily determine if the system is effective is a key symptom of this failure. This paper explored the process for development, implementation and testing of an electronic security solution. This was accomplished by asking “What is a simple and repeatable systems engineering process that promotes an effective electronic physical security system?” An effective solution was not identified within the literature review process. The Requirements, Alternative, Design, Implementation, Testing and Commissioning (RADITC) process was developed as an alternative solution for the development and validation, from requirements to testing, of an effective physical security solution. The new process is based on two existing processes. The first is a commercial best practice as articulated by Thomas J Whittle. This provides a good foundation of activities. A second more complex life cycle management process used by the Department of Defense (DoD) and Department of Homeland Security (DHS) provided steps and concepts that are missing from the commercial best practices in use today. This resulted in an effective, easy to use and repeatable process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
ASIS	American Society of Industrial Security
CCTV	Closed Circuit Television
CONOPS	Concept of Operations
CPNI	Centre for the Protection of National Infrastructure
CPP	Certified Protection Professional
DAU	Defense Acquisition University
DHS	Department of Homeland Security
DOD	Department of Defense
DOTMLFP	Doctrine Organizations Training Material Leadership and Education Personnel and Facilities
ESS	Electronic Security Systems
ICD	Initial Capabilities Document
ID	Identification
NISCC	National Infrastructure Security Coordination Centre
PCI	Professional Certified Investigator
PPS	Physical Protection System
PSP	Physical Security Professional
RADITC	Requirements Alternative Design Implementation Testing and Commissioning
S&T	Science and Technology
SAFETY	Act Support Anti-Terrorism by Fostering Effective Technology Act
SAVER	System Assessment and Validation for Emergency Responders
SPF	Security Policy Framework
UK	United Kingdom

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This paper explored the process for development, implementation and testing of an Electronic Security Solution. One way to measure the effectiveness of a facilities protection effort is to have clearly defined end users' needs and successfully test the system against those needs. The solution is only effective when you meet these needs. An Electronic Security System (ESS) is the combination of the individual electronic security components working as a single entity within a larger security plan. Some of the common electronic ESS components are video surveillance cameras, identification (ID) card readers, motion detectors with many other sensors and related software.

There are significant costs associated with security solutions. The world security services marketplace is expected to grow past the $218 billion mark in U.S. dollars by 2014 (The Freedonia Group, 2011, p. 4). By that same year, the electronic security equipment marketplace world demand will exceed $99 billion U.S. dollars (The Freedonia Group, 2010, p. 4). According to Keating (2010), by 2017, "Governments and institutions will spend $3.8 billion annually on security systems" (p. 1). In 2002 the local law enforcement community in the United States responded to 36 million calls resulting from electronic security systems with the false alarms costing an estimated $1.8 Billion (Sampson, 2001, p. 7). That translates into the equivalency of 35,000 full-time police officers nationwide doing nothing but responding to false alarms from electronic security systems (Sampson, 2011, p. 8).

There is no literature on ESS requirements as an engineering activity like those found in the software or other industries. Most security development and implementation processes begin with a variation of a survey or risk assessment and go directly into defining a set of solutions as the end user requirements. A security expert must assume what the end users security needs are within these processes or surveys. A design is then completed based on this expert opinion. The system is tested and accepted validating the design was installed properly. This results in the installed perceived solution being validated as effective and not the actual end user security needs being solved.

The Requirements, Alternative, Design, Implementation, Testing and Commissioning (RADITC) process was developed based on a common industry practice and the Integrated Defense Acquisition, Technology and Logistic Life Cycle Management System. These are requirements development, analysis of alternatives, design, implementation, test and ending with the commission of the final solution. This could be used by anyone who has basic management skills but may require an additional detailed support package for some of the steps provided by different certified professionals. All of the steps can be modified for each specific problem set or issues, but the steps themselves and the order they fall in are recommended for a successful implementation of this method. The method results in a tested system based on end-user's needs. Further validation or testing of the needs during the systems useful life can ensure the system maintains its effectiveness over time.

I. INTRODUCTION

We spend our time searching for security and hate it when we get it.
–John Steinbeck

An Electronic Security System (ESS) is the combination of the individual electronic security components in its entirety working as a single entity within a larger security plan. Some of the common electronic components of an ESS are video surveillance cameras, identification (ID) card and biometric readers, motion detectors with many other sensors and related software. Electronic security systems serve to detect and delay intruders to increase the likelihood that end users will have enough time to assess the threats and deploy responders in time to thwart an attack if needed (Sandia National Laboratories, 2012).

The English inventor Tildesley invented the first modern electronic security device in the early eighteenth century (Seungmug, 2008, p. 26). Since then, practitioners and professionals of all varieties have been looking for ways to use these new tools to solve security and life safety issues. Some of them have been looking for a problem for the newest and greatest electronic security solution to solve while others are looking to install an electronic solution because they believe not having one is the problem. Few of these experts ask exactly what does the end user need solved and how will it interact with the daily activities of the entire entity requiring a solution.

There is a limited amount of research on Electronic Security Systems, and it is unclear if the systems widely used today are providing a value compared to the cost or even increase security. A large amount of money is being expended on electronic security systems and false alarms or system malfunctions are a clear problem. This thesis focused on the process used in developing the initial needs and the solution through testing of those needs within the final solution.

Many of the practitioners in Electronic Security are self-certified experts based on years of performing the art of security and not based on any formal higher degree in security, certification or applications of scientific methods that result in a replicable

solution. As in many art forms, the expert is always right and few times do different experts with different background end up with the similar solution to the same problem.

A. THE PROBLEM

Shortly after September 11, 2001, most of the companies listed in the New York Stock Exchange lost value and some industries lost a significant percentage of business along with the downturn in value. However, companies like L-3 Communications Holdings Inc. (NYSE: LLL), URS Corp (NYSE: URS), Siemens (NYSE: SI) and Lockheed Martin Corp (NYSE: LMT) all made significant gains within the weeks and months after the attack (Google, 2012). These companies were well suited for the new burgeoning age of spending on electronic security systems. The world security services marketplace is expected to grow past the $218 billion mark in U.S. dollars by 2014 (The Freedonia Group, 2011, p. 4). By that same year, the electronic security equipment marketplace world demand will exceed $99 billion U.S. dollars (The Freedonia Group, 2010, p. 4). According to Keating (2010), by 2017, “Governments and institutions will spend $3.8 billion annually on security systems”. As seen with the problems of false alarms, the results have not drastically improved compared with the ability of the core units of these electronic systems.

Often a system will fail to meet user expectations, or even basic needs, because the supplied requirements were incomplete, inconsistent, mistaken, uninteroperable or simply unmanageable (Edwards, Flanzer, Terry & Landa, 1995, p. 278). Many issues are a result of undocumented requirements or assumptions on the part of the system designers that lead to mistaken, inconsistent, ambiguous, incomplete or forgotten requirements (Edwards, Flanzer, Terry & Landa, 1995, p. 278). Many physical security measures did not meet the users security needs because the implications of what was needed were not fully thought through (Spaight, 2000, p. 64). A good requirement should provide the link between the needs and the procurement process and they are easy to consider in principle but hard to develop in practice (Spaight, 2000, p. 64).

Many studies pointed out that poor system design; implementation, poor training and integration into daily activities are the common causes for most of the false alarms by

electronic security systems (Sampson, 2011, p. 9). A system based on a solid set of requirements that are integrated into the facility or organizational operations should overcome most of these challenges. This will increase security, lessen cost, strengthen the surrounding community and perform the missions electronic security systems are created to solve.

B. RESEARCH QUESTIONS

What is a simple and repeatable systems engineering process that promotes an effective electronic physical security system?

C. BACKGROUND

1. Physical Security

Physical security, or more specifically, the use of access controls where used as early as 1000 BC in China where a system was developed to control access to the imperial palace with different types of ornate rings (Snyder & Neil, 1989, p. 26). A physical security system refers to the protection of building sites and equipment from theft, vandalism, natural disaster and man-made catastrophes (Szuba, 1998). Physical security works best when it has more than one layer of protection surrounding a target, with each layer comprising of one or more elements (Gordon & Wyss, 2005, p. 7). These elements can be physical structures, processes, people or ESS.

Physical security measures aim to detect and possibly prevent a direct assault on premises or reduce the potential damage and injuries that can be inflicted should an incident occur (Center for the Protection of National Infrastructure, 2012). Having a security solution is deterrence. An overall physical security solution is comprised of three major functions: detection, delay and response. A key item within detection is Electronic Security Systems (U.S. Army Military Police School, 2001, p. 6-1).

Electronic security is a key element of physical security. The modern electronic systems provide increasingly better system design possibilities for varying applications, improving with the growth and expansion of the commercial electronics marketplace. Recent technological advances provide advantages such as new capabilities, faster

detection and response rates, greater ease of operation and lower error margins, thereby offering better security (Hoffman, 1989, p. 74). These are fundamental ingredients to all security efforts. Without this foundation of electronic security systems, security can be considerably more difficult, if not impossible, to effectively implement.

D. PERFORMANCE ISSUES

The base technology of electronic security systems has followed the growth of communications and Internet Technology. This has revolutionized security systems design, detection, communications and monitoring abilities. Technology continues to advance and will continue to foster new electronic security capabilities. Detection equipment continues to develop as well, with more sophisticated devices and more reliable sensors providing better sensitivity and greater security abilities (DGA Security Systems, 2012, p. 1). ESS leverages the growth in consumer electronics, and this increase in capabilities and reliability should provide these same increases in the electronic security applications and results.

1. False Alarm

False alarms are also known as nuisance alarms, false activation, false dispatches, false trigger or unknown alarm activations. False alarms are those created by electronic security systems that do not show an actual or attempted intrusion (Ohlhausen Research I, 1993, p. 6). False alarms comprise 95 to 98 percent of all alarm calls to police dispatchers (Ohlhausen Research I, 1993, p, 6). In 2002, the local law enforcement community in the United States responded to 36 million calls resulting from electronic security systems with the false alarms costing an estimated $1.8 Billion (Sampson, 2011, p. 7). That translates into the equivalency of 35,000 full-time police officers nationwide doing nothing but responding to false alarms from electronic security systems (Sampson, 2011, p. 8). Mark Twain made it clear in his 1880 short story, *The McWilliamses and the Burglar Alarm* that false alarms were already well-known attributes to even the early electronic security systems (Twain, 1922).

2. Engineering Process

There are many process, best practices, standards and models that exist that describe what is commonly known as a design or development process. These all have different naming conventions but are basically a form of an engineering process that essentially details how electronic security systems are designed and implemented. The Systems Engineering Process, displayed in Figure 1, is a Department of Defense comprehensive, iterative and recursive problem solving process, for transforming needs and wants into a set of system product and process descriptions. (DAU, 2001). This is a typical engineering process. This process typically begins by identifying the problem and associated stakeholders. The problem is then properly defined and refined to ensure it properly describes the customer's needs (Letourneau, 2009, p. 8). These are documented in the needs document and are used as a baseline for the entire design and development effort and become the eventual goal of the system under consideration. In the simplest terms, this seeks to take what the customer wants and needs through a methodical process, eventually providing them with a product or process definition that meets the needs at a given level of development. Following a predefined process to design, development, implement and test any major or important system is a common, if not required, best practice.

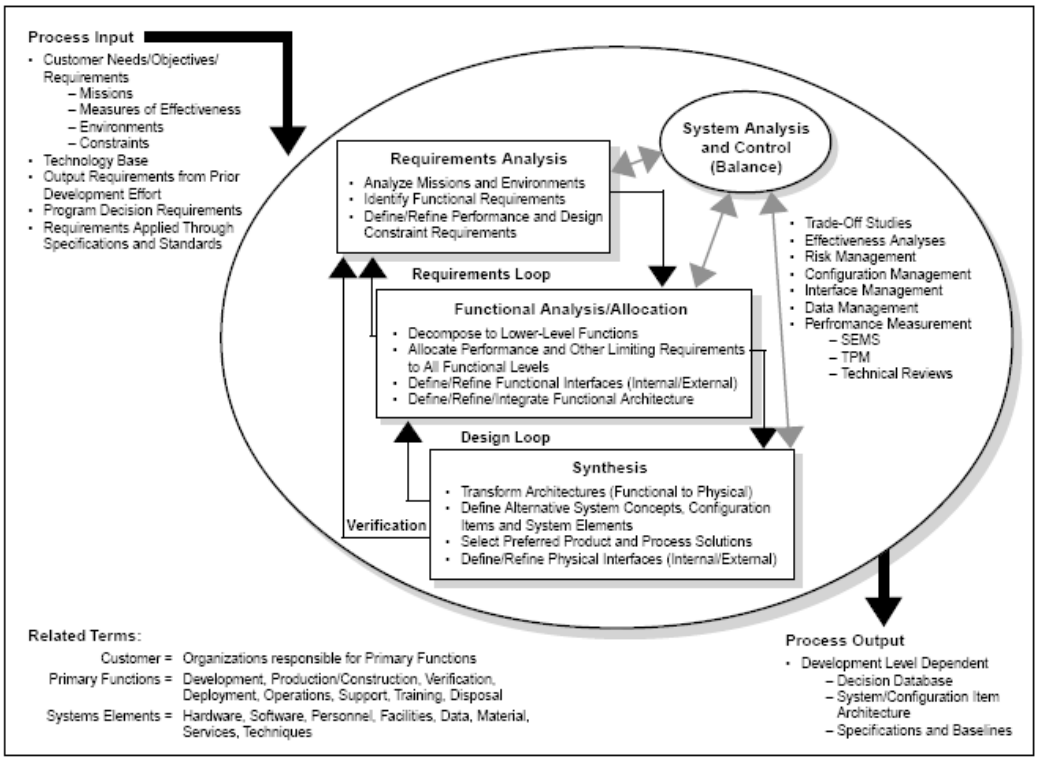

Figure 1. Systems Engineering Process (From DAU, 2001)

II. LITERATURE REVIEW

> *Look for something, find something else, and realize that what you've found is more suited to your needs than what you thought you were looking for*. –Lawrence Block

There are a number of academic studies on gathering requirements in many disciplines. The literature around system development for electronic security is limited. The review looked at how the ESS industry defines what an expert is, what requirements are along with a look at a couple of different representative approaches to ESS. These representative best practices are from Sandia National Labs, the United States Departments of Homeland Security and Defense along with The United Kingdom.

A. DEFINING ELECTRONIC SECURITY EXPERTS

Industrial security practitioners charged with government-mandated protective measures for military critical commercial infrastructure created the American Society of Industrial Security (ASIS) in 1955 (Seungmug, 2008, p. 20). They currently advertise over 38,000 members and 200 local chapters worldwide on their website, www.asisonline.org. In 1972, the organization concluded that industry credentials are required, if the vocation or art form of security was to become a profession (ASIS, 2012). After approval of the Department of Defense, the organization created the first board certified designation and certification program. The certifications from this program were awarded the Department of Homeland Security (DHS) designation under Support Anti-Terrorism by Fostering Effective Technology (SAFETY) Act of 2002 and are accredited by the National Standards Institute (ANSI) (ASIS, 2012).

Now known just as ASIS International, this organization has developed three industry certifications. The original certification provided is the Certified Protection Professional (CPP), and it is for security managers. The other two board certification designations started in 2002 (ASIS, 2012). The Professional Certified Investigator (PCI) is centered on private investigators. The Physical Security Professional (PSP) board certified designation is centered on those in the field who have a primary responsibility

for physical security assessments, the application, design and integration of physical security systems and measures (ASIS, 2012). Less than nine thousand individuals worldwide have met the minimum requirements and have been awarded one or more of the three board certification designations under this program (ASIS, 2012).

There is a large number of training and certifications available from the manufactures of the electronic security equipment. As an example, Pelco by Scheider Electric maintains a global training institute that maintains a virtual, along with several brick and mortar campus and provides an onsite technical training service (Pelco, 2012). They are a large traditional security camera manufacturer and have certifications to support sales and design teams within the entire product suite along with individual product specific certification and training for the technical installation and service teams. This is typical for most of the major equipment manufactures. These product certifications are normally required by the manufactures for the design and installation companies to purchase equipment, maintain the manufacturers warranty and support provided by them.

Many industry ESS experts present these individual product certifications as evidence of industry or market knowledge. In fact, these are limited to the specific manufactures or individual product lines of a single manufacture. Too many practitioners use this limited knowledge base and the prevailing processes that reply on them to develop sound security solutions. This easily results in the solution meeting the capabilities of the manufacturer's features the individual has been certified on and not on the actual needs of the end user.

B. ELECTRONIC SECURITY REQUIREMENTS

A significant amount of time and work can be saved if an expert jumped straight to the solution without defining the problem. If shortcuts are taken, the solution may not be the best choice among possible alternatives or, even worse we are likely to find that the solution does not solve the problem, if not make it worse (Cellucci, 2008, p. 8). Gathering the correct requirements from all the stakeholders of a system is so important to Congress for the Department of Defense (DoD) that oversight councils and other

related activities have been codified in law under 10 U.S.C. 181 and other acquisition related laws and regulations regarding the development of new systems (Cornell University, 2012, p. 1). The DoD defines a requirement within the acquisition process as a statement that defines a product or process operational, functional, or design characteristic or constraint, which is unambiguous, testable or measurable, and necessary for product or process acceptability (Defense Acquisition University, 2008). Such a requirement is considered a crucial component to understand what a system design should accomplish.

A common and basic definition for a requirement is something that is needed (Oxford University, 2012). In practice, there are many different types of requirements that all fit within this larger definition. It may also be said that a good requirement will be correct, feasible, necessary, prioritized, unambiguous, verifiable and solution agnostic (Wiegers, 1999). Some of the more common types are: functional, performance and operation (Project Performance International, 2011).

Functional requirements state what the system should do (Halligan, 2012, p. 2). This captures the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform (Malan, 2012, p. 2). In the security context, functional requirements may state the need to identify users entering a specific room or location.

Operational requirements identify the essential process or series of actions to be taken in order to address mission area deficiencies, evolving applications or threats, emerging technologies, or system cost improvements (Mitre, 2012, p. 1). These typically involve integration with the Concept of Operations (CONOPS) of the location under consideration. An example of an operational requirement could state the need to ensure the proposed new system does not increase labor force cost over the current staffing models.

Performance requirements state how well the system is to complete the desired task (Halligan, 2012, p. 2). A performance requirement is generally defined in terms of degree, rate, quantity, quality, timeliness, and so on (Argospress, 2012, p. 1). A good

example could list the accuracy of detection and in the security context to require the security design to ensure that the detection rate at the entrance shall be 100 percent accurate.

A good security requirement will include the characteristics of many different types of requirements but not include the solution or technical characteristics of a proposed solution. Technical characteristics within the solution will not facilitate technical and nontechnical alternatives when looking for a final resolution. The solution is defined after all of the requirements have been identified and validated in any standard system engineering or design process. A solid security requirement for an entrance to a room may read: There is a need to identify all individuals entering this specific area with a 100 percent detection rate, accurately capture the date and time of entrance, incorporating the current security identification process used at the facility while not increasing current staffing levels.

C. ASTM

ASTM International (ASTM), formerly known as the American Society for Testing and Materials, is globally recognized for the development and maintenance of standards. ASTM defines a specification as an explicit set of requirements (www.astm.org). A specification may contain a system design and architecture but these are not interchangeable documents. They typically categorized requirements in two distinct groups as functional and nonfunctional. Functional requirements capture the intended behavior of the system (Bredemeyer Consulting, 2012). This would answer the question: ”What should the system do?” Nonfunctional requirements captured the criteria that can be used to judge the operation of a system (Malan, 2001). This answer the question: “What should a system be?” Good clear sets of requirements are the foundation of any security system.

D. SANDIA NATIONAL LABORATORIES

Sandia National Laboratories is recognized as a center of excellence related to physical protection systems by the Departments of Defense and Energy. The Laboratories are managed by the Sandia Corporation and is a wholly owned subsidiary of Lockheed

Martin Corporation. They have a mature process for system design and evaluation that was first developed to protect nuclear assets. This process is used as the reference for many current practices and concepts related to securing a fixed location against physical threats. According to Sandia, "A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks" (Garcia, 2001, p. 1). An Electronic Security System (ESS) is a significant component within a physical protection system. Figure 2 shows the Sandia process that follows a three-step process: Determine the PPS objectives, design the PPS and analyze the design.

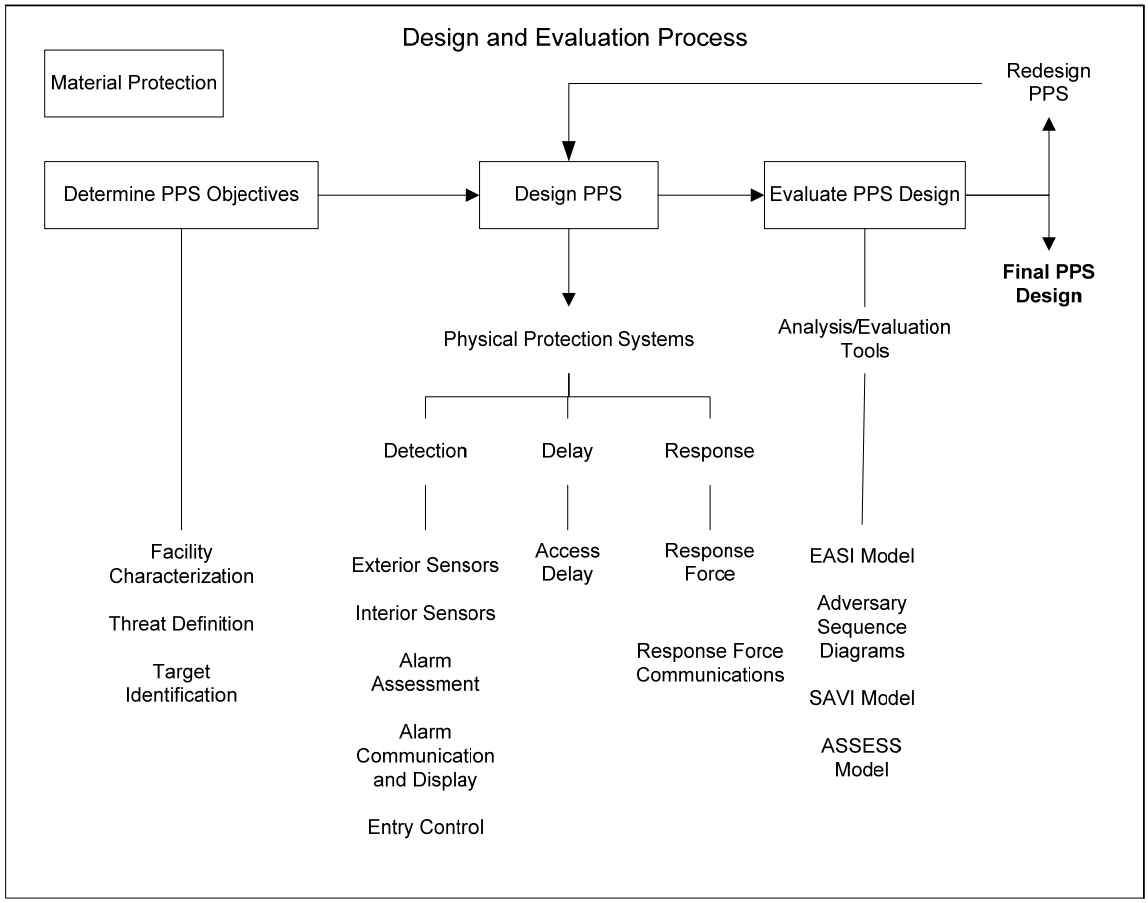

Figure 2. Sandia Process

Determining the PPS objective is the closest step in the process that determines the requirements for the security solution. This initial step requires the understanding of the facility. This is completed by a review of the facility design, layout and construction

along with any other operations or conditions that may affect the physical protection system. The next two steps described in Figure 2 appear relatively straightforward. Determining the threat and determining what potential targets may exist in the facility. All these factors combined are used to help design the PPS. There is no step in this process to specifically identify and document requirements. There is an implied assumption in many of the associated writings that the determined objectives process provides the necessary requirements without specifically identifying them as such. This is based on the next step of the process being the actual design of the PPS. Any design process needs a baseline requirement of some order to be a relevant design or solution. At no time does the process verify the system works as required.

This process works well for a highly technical and capable security team that is highly trained, certified and working within a controlled environment. It assumes the design team can define the end users need and successfully incorporate them into the systems objectives based on observations and not interactions or actual input from the end users or other stakeholders. A possible solution to mitigate this could be the addition of something associated with the generation of the end users needs that would be the foundation of the PPS objectives along with other security related activities. The needs identification step is not defined and no artifacts are provided that clearly delineates the system's ultimate goals. The process goes right from gathering generic background and location information into system design with no ability to determine success or whether actual needs are met and incorporated into the facilities daily operations.

E. THE DEPARTMENT OF HOMELAND SECURITY (DHS)

The United States Department of Homeland Security has several activities that are relevant to a methodology for determining and validating requirements. The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology (S&T) Directorate of DHS, the SAVER Program conducts objective assessments and validations of commercial equipment and systems and provides those results along with other

relevant equipment information to the emergency response community in an operationally useful form (U.S. Department of Homeland Security, 2012, p. 1). SAVER Reprints are reports produced by the Department of Homeland Security and can be found at https://www.rkb.us/saver/.

One of the SAVER reports titled *CCTV Technology Handbook* has a chapter on system design. The report uses terms like functional and operational requirements (SPAWAR, 2006). "Once the surveillance or access control functional requirements are identified, the operational requirements must be analyzed in detail to define what information the system will be expected to provide under the existing operating conditions (SPAWAR, 2006, p. 5)." Although these terms are used throughout the document, they are not defined, described or used in a means that allows the reader to understand what they are and how to create them. These reports are considered industry best practices and include the applications of some electronic security technology.

F. THE DEPARTMENT OF DEFENSE (DoD)

The Department of Defense (DoD) has several documents related to electronic security systems applications and requirements. These are a compilation of the current best practices and mandates associated with electronic security systems. The largest both in size and use is the FM 3-19.20 *Physical Security Manual*. This is referenced by many internal and external organizations and is intended to be the one-stop physical security source (U.S. Army Military Police School, 2001, p. vi). It has a focus on an effective partnership between engineers and physical-security personnel (U.S. Army Military Police School 2001, p. 3–1). They view the separation of roles as a good concept for the development of requirements and the design of the system. This is important because is distinguishes that there are different roles and skill sets required between the development of requirements and the design of a system. The manual describes the Army policy that the use of standard preapproved systems, if possible and available, as the preferred method (U.S. Army Military Police School, 2001, p. 6–1). This is important, since the preapproved systems are based on technical ability, not operational need. In effect, they have a predefined solution looking to fit all of their electronic security needs.

The end users of the Army manual will find the implementations of these systems are based on general requirements tailored to a site-specific mission and physical profile (U.S. Army Military Police School 2001, p. 6–2). The determination on what makes up a site-specific mission and profile begins with a site survey. For this effort, the manual describes the inclusion of such factors as terrain, geography, climate and type of assets needing the security (U.S. Army Military Police School, 2001, p. 6–2). These are clearly components of the design criteria that an engineer should take in consideration for the system design. These depend solely on the skill set of the practitioner and not the process itself.

The United States Marine Corps *Physical Security Program Manual*, MCO P5530.14 provides the guidance they use relating to physical security and includes electronic security systems. They view these as consisting of sensors that signal the entry or attempted entry into a protected area, not the prevention of an entry (Headquarters United States Marine Corps, 2000, 7–3). The manual determines who is responsible for the system but not specifically how the design and implementation shall be completed. Overall, this provides little guidance on how the system will be designed and operated but has a focus on who is responsible for these processes.

G. UNITED KINGDOM

The United Kingdom formed the Centre for the Protection of National Infrastructure (CPNI) from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC) on 1 February 2007 (Humberside Police, 2012). The Centre enables national security for the United Kingdom by providing security advice and guidance (Centre, 2010, p. 4). They support physical, personnel and cyber security efforts. The Centre advocates the production of Operational Requirements, and they are within the United Kingdom’s Security Policy Framework (SPF). These requirements are based on a process that has been successfully applied across the UK national infrastructure (Centre, 2012). They published a guide titled *Guide to Producing Operational Requirements for Security Measures*. This defined an Operational

Requirement as a statement of need based upon a thorough and systematic assessment of the problem to be solved and the hoped for solutions (Centre 2012).

The Centre's guide is designed to ensure the appropriate security measures are used to manage risk by the use of an electronic security system (Centre for the Protection of National Infrastructure, 2010, p. 2). They describe how to develop Operational Requirements and how they are broken down into two levels. Level One Requirements are based on the overall security needs and level two are more at the component level. In basic terms, a Level One Requirement would be an entire campus or facility area. A Level Two Requirement for the same location would be a specific solution within that higher Level One Requirement. The example used in the guidance document for a Level Two Requirement is a specific fence, video surveillance or access control. These require you to have a complete understanding of the threats to that particular campus or facility prior to completing the Operational Requirement generation process.

The generation process is initiated when a security problem has been identified, and it is understood why it has occurred. The process end-user is asked six questions, and if yes is answered to one or more of the first five, then a Level One Requirement is developed. These are:

Are the existing security measures inadequate?

Are the existing security measures excessive?

Has the use of the location changed?

Has the threat changed?

The current requirements are not clear?

If you answered no to all of the above and/or you can state the existing security measures are considered to be appropriate and adequate, then no action is required and the process ends.

The actual development of the Level Ones Requirements requires the input of every stakeholder. The Centre's guide defines stakeholder as anyone who has any interest in the locations security (Centre for the Protection of National Infrastructure, 2010, p. 4).

Everyone is provided a prefabricated checklist of questions design to ensure they have some level of input into the development of the requirements. They are asked to describe the location, assets, threat, concerns or vulnerabilities, consequences, definition of success, other constraints and possible solutions. These are all combined into summaries that are the Level One requirement for that location.

Level Two Operational Requirements are framed around eleven predetermined solution sets. The sets are: Pedestrian barrier, lighting, video surveillance, physical delay measures, procedures, information security, hostile vehicle, perimeter intrusion, access control, intrusion detection and mail. Each one of these areas has their own prefabricated checklist for the stakeholders to complete. These checklists cover topics from areas of concerns, functions and vulnerabilities to constraints, success criteria and maintenance issues. As in the higher-level Operational Requirements, the summaries of all the stakeholders' surveys for each Level One end up as the final Level Two Operational Requirements for the facility

When broken down, this process is a little different from the checklist concept used by other entities in the United States. The UK requires the actors in the process to be well versed in the systems used and types of applications. This becomes a problem when they are only versed in one technology, or one manufacturer, or have limited to no prior experience in the engineering of these systems. Some of the benefits of this methodology are that the definition of success for the Operational Requirements is a core component, and that it does not heavily rely on a single individual for that single point of failure.

H. SUMMARY

There is a lack of agreement on defining a requirement and the ways to create them. An extremely limited amount of relevant academic literature was found associated with the Electronic Security marketplace. There is no formal ESS field of study on requirements as an engineering activity like those found in the software industry. Most processes begin with a variation of a survey, or risk assessment, and go directly into defining a set of solutions as the end user requirements. There are a small number of board certified experts actively working in the ESS field. These experts must assume

what the end users security needs are based on surveys or risk assessments. This results in the system being tested and accepted validating the design based on experts' perceived solutions as installed and not against the actual end user's security needs being resolved. The federal government's integrated life cycle management system is considered complex for the average federal user of the system and will not easily support an activity like an ESS solution.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHOD

The only real security that a man can have in this world is a reserve of knowledge, experience and ability. Henry Ford

An overall physical security solution is composed of three major elements: detection, delay and response. Electronic Security Systems are the key components within the detection and delay elements. These are normally integrated systems comprised of Closed Circuit Television (CCTV), intrusion detection, access control and other electronic means of detecting access and intrusion within a defined location. There are five life cycle phases that make up these systems and all are crucial to quality. These are the development of the requirements, design, implementation, operations and maintenance of these systems.

This thesis developed a requirements process tailored for the development and testing of an ESS. The desired goal of the analysis was to develop a process that is effective, easy to use and repeatable.

A. DEVELOPMENT OF MODEL

The new requirements process was based on two existing processes. The first is a commercial best practice as articulated by Thomas J Whittle (Whittle, 1987); the second is commonly known as the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System. Both of these are important foundational process.

Thomas J Whittle, PE shared a version of this common industry practice in his April 1987 article called security by design in Security Management (Whittle, 1987, p. 57). The checklist or survey methods used by industry are this methodology or a slightly modified version. These are the basis for many of the commercial applications in use today.

The Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System is the DoD and DHS Systems Acquisition Process. This is the process these agencies follow when they need to develop, purchase and maintain

everything from the largest nuclear aircraft carrier to the employee identification card (The Defense Acquisition University, 2009). This is based on the Defense Acquisition Guide and is a very complicated process to follow. Figure 4 is a roadmap of just the key activities within the systems acquisition process (The Defense Acquisition University, 2009). Both of these are key components in the development of a new process.

The new process included steps to determine the needs, develop a solution and ensure the needs are captured within the final solution. My personal experience played a key role within the development process of this new process. This experience includes more than twenty-seven years within the defense and security field. Within those years, I have held executive, program management and project management and team leadership positions. I have successfully developed and led security-related assessments, designs, processes and teams in both the government and large industry applications. I have served as the primary decision maker on the design and management of many successful large-scale security products and systems with real world hands-on experience. I currently maintain a level three certification in program management within the Department of Homeland Security and a board certification as a Physical Security Professional.

B. DESIRED CHARACTERISTICS

Desired characteristics for the new process are: simple, repeatable and effective.

1. Simple

Simple is the determination on the ease in which the process can be implemented free of secondary complications. A simple process will be easy to use with no specific process based training required. This will be determined by the complexity and the clarity of the steps provided. This will have a direct path between each point in the process when displayed as a figure. Each step will have a clear meaning and task. This is a key characteristic, since the average security professional will not use the process more than a couple of times over an entire career, training or consultants are costly. Most solutions are expensive and can take years to implement with at least a five-year useful life after implementation.

2. Repeatable

Repeatable represents how well a practitioner can apply this same process in multiple environments. Process repeatability is the foundation for the operation of a successful process. In order to measure the success of a process, it needs to be repeatable. Otherwise, there is nothing consistent to measure and compare. To be able to measure process improvement, repeatability is essential. So, repeatability is a critical factor in continuous improvement and the ultimate success of a process. The types of environments a successful process should work include school campus, office buildings and small manufacturing facility. Not only should the process be location agnostic, it needs to be solution agnostic. Having a process that will direct a solution into a single technology is not dynamic or repeatable. The process will fail if that solution it provides is not viable in the environment the process is being applied to. In this context, a process that is location, technology and solution agnostic is considered to be a repeatable process.

3. Effective

Effectiveness refers to the level of ability of the method to obtain testable end user requirements and test the proposed electronic solution against them. The validation that a system is effective can be done by testing it against the user needs, ensuring it is integrating into the daily activities of the end users to improve the chances and opportunities it will be successfully used. The process should clearly define requirements by supporting the identification of the end user needs. This will facilitate the proposed solutions integration within daily activities to ensure the solution will be utilized. It shall test the solution directly against the identified needs.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ALTERNATIVE DEVELOPMENT

> *We will bankrupt ourselves in the vain search for absolute security*.
> Dwight D. Eisenhower

The method used to take an electronic security system from the basic needs of an end user to an effective system is important. It is highly possible that a large amount of time and money can be allocated to an ESS resulting in an unknown, little or no real amount of value. The new requirements process was based on two existing processes. The first is a commercial best practice as articulated by Thomas J Whittle. This provides a good foundation of activities. A second more complex life cycle management process used by the DoD and DHS provided steps and concepts that are missing from the commercial best practices in use today. This life cycle management process is commonly known as the Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System.

A. COMMERCIAL BEST PRACTICE

Interviews, site surveys and other customer interactions are all components of the best practice in industry to develop and validate requirements in the electronic security field. As shown in Figure 3, Thomas J Whittle, PE shared a version of this common industry practice in his April 1987 article called security by design in Security Management (Whittle, 1987). Versions of this are found in many best practices used by security professionals and are known as the checklist or survey method.

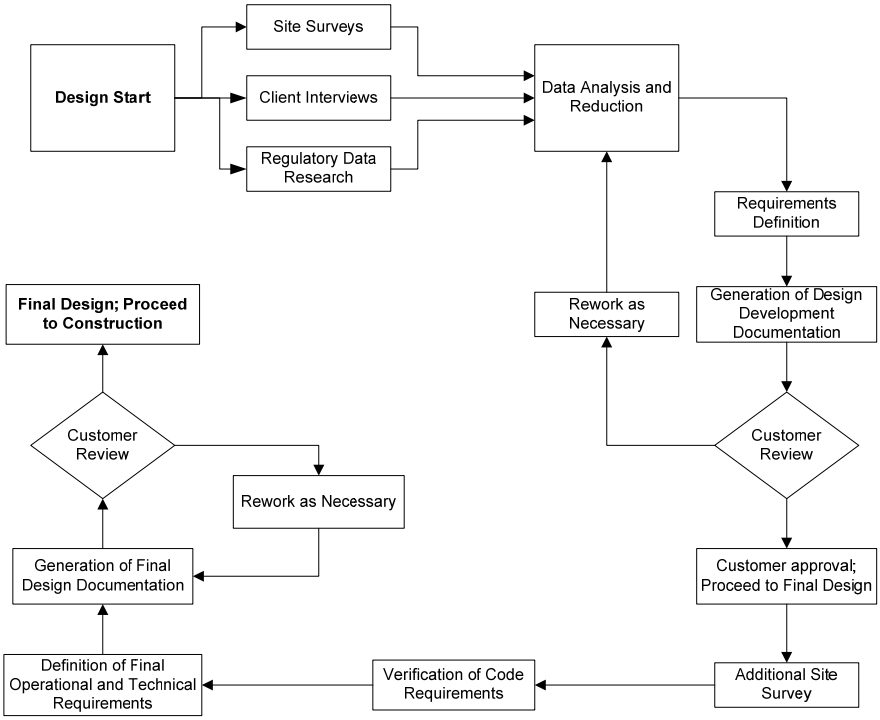

Figure 3. Commercial Method

Having a clear understanding of the customers and end users perspective are key to this method. What is not shown in the figure is the inclusion of customer questionnaires to help prepare for the client interviews. None of the proposed interview questions or missing steps to prepare for the interview is publicly available. Although not specified it could be easily inferred that these are specific to the expert conducting the task along with the nuances associated with the environment requiring some level of security. Most relevant documentation heavily relies on the expertise and opinion of the user completing the development of the requirements and design. This process stops at the beginning of the installation phase of the project. At this time, there are still many activities and events that will determine how well the system will function. It is clear that a well-designed system not installed properly will not be as effective as one that is installed properly. One of the ways to verify the system works as designed is to test the system after installation.

According to Mr. Whittle (1987), a detailed site survey that includes environmental and operational factors plays an important role on the design of a system.

He also advocates a regulatory data search. All of this collected data should then be analyzed or reduced to the basic important facts to use toward the design of the system. The process, or what the results look like, makes it difficult to understand this step in the process. At this point in the process, the development of the requirements is completed and forms what he called generic requirements. These are used for the systems design, and the process moving forward to include customer feedback and additional surveys.

B. LIFE CYCLE MANAGEMENT SYSTEM

The Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System is the DoD and DHS Systems Acquisition Process. This is the process these agencies follow when they need to develop, purchase and maintain everything from the largest nuclear aircraft carrier to the employee identification card (The Defense Acquisition University, 2009). This is based on the Defense Acquisition Guide and is a very complicated process to follow. Figure 4 is a roadmap of just the key activities within the systems acquisition process (The Defense Acquisition University, 2009). This is a good graphical representation on how complex this process is.

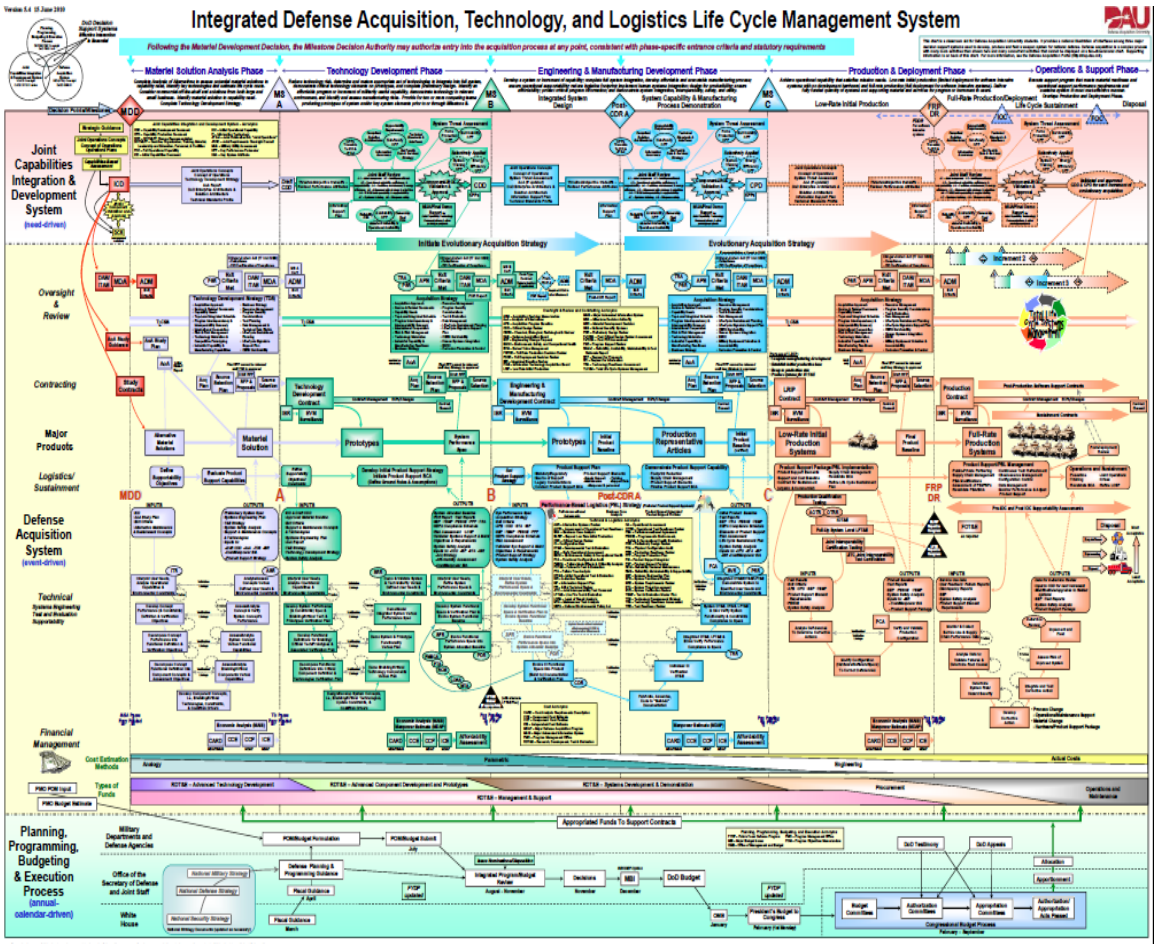

Figure 4. Life Cycle Management System

This large and complex life cycle management system can be broken down into five phases. The five phases are: Material solution analysis, technology development, engineering and manufacturing, production and deployment and operations and support. This is too complex to be directly adapted to any ESS implementation. This was developed specifically for the United States federal government and the required continual checks and balances to ensure there is a cost effective functional solution with as little waste fraud and abuse as possible.

According to the Defense Acquisition Guidebook (DAU, 2009), the material solution analysis phase is the first phase a need enters the acquisition system. Prior to this phase an Initial Capabilities Document (ICD) is created that details all the capabilities any proposed solution would need to satisfy under the current need. That means that the

end user has to have a clear set of requirements on what is needed prior to even starting the acquisition process. The requirements are developed by the end user communicates within the framework of the ICD document template. The material solution analysis phase will complete an analysis of alternatives, or determine what are all the viable solutions to meet the mission needs. At this point in the process, the government determines the estimate cost of the system, a development strategy, contract drafts and plans, system technical specifications, engineering plans, support plans, cost manpower estimates and other early supporting documents and decisions.

The second phase is the technology development phase. This is the point in the process that the performance parameters are determined that the solution must meet based on the initial requirements. Technical performance specifications are developed and prototypes of the solution may also be found within this phase. This is the phase a design is completed, performance specifications are finalized and validation of the proposed solution will meet all the user needs. When this phase is complete, the solution will be ready for production.

The engineering and manufacturing development phase is next. This is the step that entails all of the subprocess getting a solution from an early prototype to early production runs. This is the phase the solution is integrated into the regular field operations, training and how it will be supported is determined. The integrated system design is completed and any prototype is updated to produce what the baseline solution should look like. An initial production run may take place to ensue the proposed solution can be built to meet all of the user specifications. Manpower affordability and life cycle cost are all updated. The solution is ready for full rate production at this time.

The production and deployment phase starts with a low rate or initial production run of the solution and support packages are built to ensure the solution can be successfully integrated and maintained by the end user community. A full package of support and training material for both field operations and maintenance is delivered prior to any solution being provided to an end user. This initial low rate production at the start of this phase not only provides the knowledge on how to efficiently produce the solution but also provides the knowledge and solution components to complete the training

development and implementation for the end users and maintenance personnel. Training prior to the solution arriving in the hands of an end user is important to ensure they know how to safely use it once it arrives but also how to start the initial preventative and operational maintenance on the solution that will be required.

The final phase is operations and support. This is the only time in this life cycle management system that two phases may be concurrent. This starts as soon as the first production solution is provided to the first end user. This is nothing more than the operations and maintenance of the solution. It is normal to have a solution in the hands of some of the end users and production of the solution to continue for a long time. This is continued unit the last step of the life cycle management system, solution disposal.

C. ALTERNATIVE PROCESS DEVELOPMENT

Technology is in a constant state of growth in capabilities and affordability. According to Keating, by 2017, “Governments and institutions will spend $3.8 billion annually on security systems” (Keating, 2010). By that same year, the electronic security equipment marketplace world demand will exceed $99 billion U.S. dollars (The Freedonia Group, 2010, p. 4). As seen with the problems of false alarms, the results have not drastically improved compared with the capability of the core units of these electronic systems.

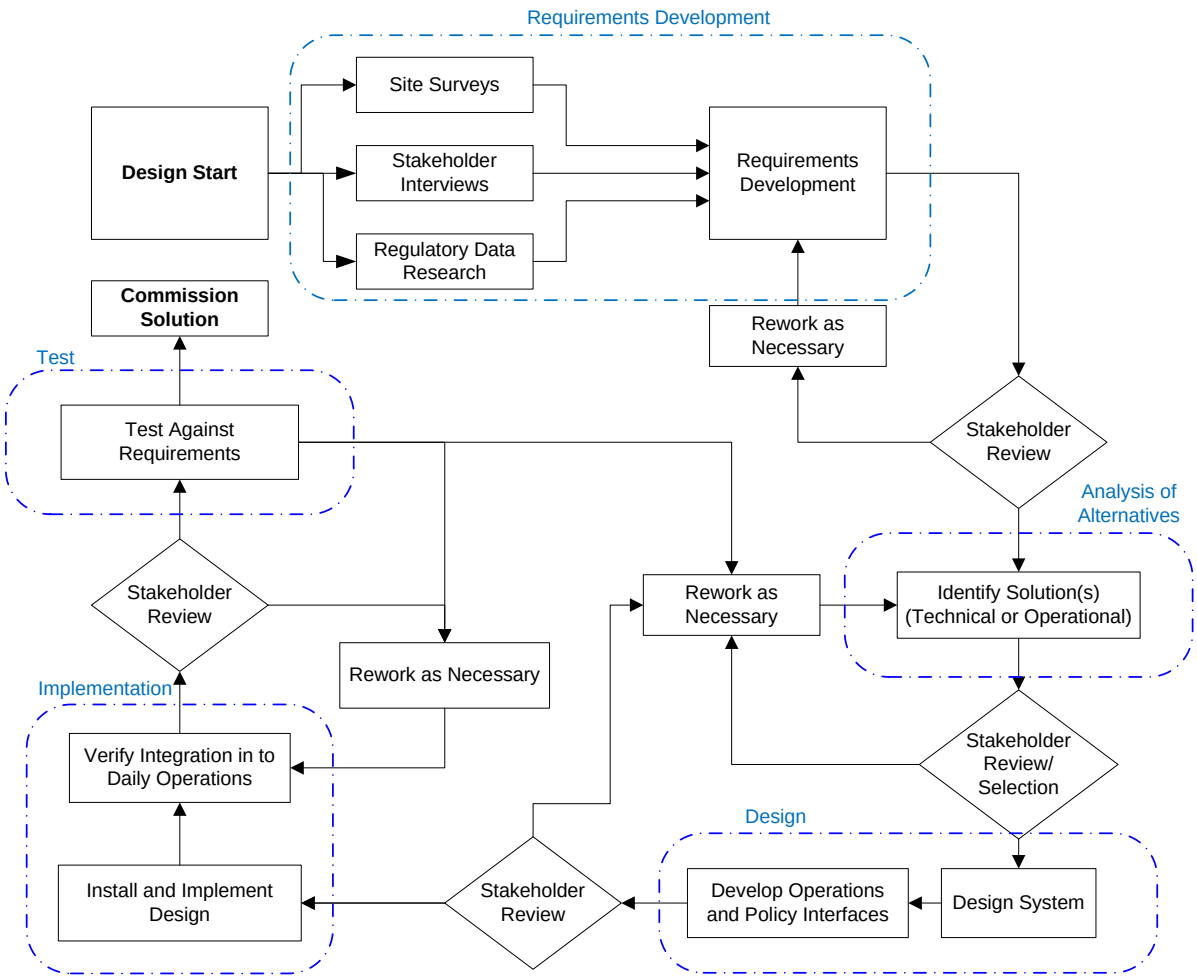

Figure 5. RADITC Process

The Requirements, Alternative, Design, Implementation, Testing and Commissioning (RADITC) process was developed as an alternative solution for the Development and Validation, from Requirements to Testing, of an effective physical security solution. The RADITC Process in Figure 5 can be broken down into six major activities or phases. The process takes its name from those six major activities. This new process is an adaptation of the Integrated Defense Acquisition, Technology and Logistics Life Cycle (acquisition) Management System used by the DoD and DHS to acquire new solutions along with the commercial option. The six phases of the alternative process fits within the federal acquisition management system and the commercial option provides a good foundation for this new process.

1. Requirements

The requirements development phase takes the beginning of the commercial option and expands it to include a well-defined result of end user requirements. This uses the same “rework as necessary” steps used in the commercial option but expands the use for each phase of the process to facilitate the validation of the solution at multiple times. This phase of the alternate solution provides the valid end user requirements. A solid set of end user requirements is a key input into the federal life cycle management system.

Maintaining the commercial solutions approach in using the location (site surveys), end users inputs (client interviews) and local laws (regulatory data research) are important factors in determining if any proposed solution can be viable in the environment it will be used. This is the foundational data for any good set of requirements. What is changed from the commercial option is the next step of data analysis and reduction into actual requirements development. The generation of a good requirement is not data analysis but the generation of new data as well defined needs based on the information gathered to this point.

The requirements development phase can be split into the data collection and the development itself. Data collection includes surveys of the location, environmental and operational conditions along with stakeholder interviews and knowledge of the regulatory requirements. These will provide all of the data required to understand what the root problem is, how a solution will fit within the operations and what conditions will impact any proposed solution. The regulatory data search is a key component. Many of the security related issues have relevant local, state and national regulations associated with them along with most of the possible solutions. There is also a significant amount of domestic and international codes and best practices that may provide justification for or unidentified possible solutions.

The requirements themselves should not indicate a solution. This need to have a solution agnostic approach to the requirements will help ensure you have identified the actual problems and not just a solution looking for a home. A poor requirement could be: “have a camera looking at an entrance to the facility.” The actual requirement may be the

need to recognize anyone entering or leaving the facility at any given time. A guard with or without a mix of other technologies could also solve that same problem at a lower cost or better fit within the current constraints and operations at that location. Limiting the implementation to a specific solution as a requirement will limit one's ability to ensure the actual issue has been solved and with the best methodology within the operational constraints of the location.

Once solid sets of requirements have been created, they should be vetted by all of the stakeholders. This will help ensure that the data gathering activities did not miss anything, or there were communication issues on what the actual root problems are. This gives the stakeholders a second chance with a new perspective to ensure they have identified all the needs and have not missed any or exaggerated them earlier in the process. This leads to the identification of possible solutions.

2. Alternative

The material solution analysis phase is the first step in the federal acquisition system. This includes the analysis of alternative process that assesses the potential material and nonmaterial solutions in meeting the end user needs (The Defense Acquisition University, 2009). This step is not found in the other two processes. This was added as the next phase in the alternative solution after the development of the requirements. The DoD uses the DOTMLFP problem-solving construct to complete the analysis of alternatives. This problem-solving construct is further explored in the last chapter of this paper. As an example, a good set of alternatives for the requirement to recognize individuals entering a specific room could be the use of closed circuit television, posted guards at the entrance, sign-in sheets, electronic access control system or local personnel always staffing the room doing a visual check of all identification cards.

Having the choice between mutually exclusive possibilities will improve the chances that the solution provided from the use of this process will meet the end users needs. It is also important to recognize that even in a process to develop an ESS that a policy change or other nontechnical solution may provide better results for the end users.

This step will not only provide alternative solutions that may be operationally or cost effective but will also validate the original set of requirements developed by the process are as accurate as possible. A good indication the requirements are not clear is a lack of nontechnical or a limited set of technical solutions developed by the process, no matter how cost or operationally effective they may be. The best possible solutions or set of solutions should be presented for stakeholder review within the solution selection process.

3. Design

The next phase in the alternative solution is design. This includes the actual design of a solution and the development of operational and policy interfaces to this solution. This follows the general concept in the engineering and manufacturing development phase of the federal acquisition system that ensures the solution can be successfully integrated into and maintained by the end user community. This is a missed step in all of the existing processes and is a key to the successful deployment of a solution in the federal acquisition system.

The design phase is split into two major functions. The first is the actual design to the accepted solution, and the second is the development of the operational and policy interfaces. These are both key and should be done as close to each other as possible. These are within the same phase because these functions are not only closely related but are dependent on each other. A solution should be designed to facilitate the implementation into the daily activities and a part of the regular operations of the location under consideration. The solution must not only provide the desired security capabilities but be used to be effective.

4. Implementation

The implementation phase is next. This includes the actual implementing the solution and validation the operational and policy interfaces between the end users and the solution. The validation of the proposed solution is not part of the commercial model but key in the larger DoD/DHS acquisition framework. The validation of the successful

application of the operational and policy interfaces developed in the last phase is the next logical progression in the process. This does not define a solution is a success—just that it is being used within the daily process.

Implementation involves the actual vendor selection, purchase and installation of the proposed solution developed earlier in the process. This will also include the application of the process and activities that have been developed into the regular activities of the end users to ensure the solution is used. A proposed solution and design may change when actual products and vendors are selected and as the solution is being installed. This is a result of conditions that may have not have been known prior to this phase of the process. These changes will happen if only on a small scale with little to no impact on the proposed solution but should be tracked to ensure that any impact they have is mitigated prior to the solution being accepted. The installation of a technical solution by electricians, low voltage technicians and possibly other construction trades is a key component in the long-term viability of the proposed solution and should not be done with little to no supervision and third party verification. Small changes made by these professionals in the installation phase can have a drastic impact on the operational efficacy of the solution that may not be visible to the installers.

5. Testing

The last phase commonly used in the development of an ESS is testing the system against the design to ensure the system was completely installed and any changes from the design are clearly identified. This is the second to the last phase of the RADITC process. This is testing against the initial requirements and not against the design or implementation of the design into the daily activities. Testing against meeting the initial requirements is the acceptance component within the federal acquisition system and is the final step prior to commissioning the solution. The testing against the actual requirements is the final effort that a solution is provided that meets the needs and is actually used on a regular basis. Typically this can be accomplished with a checklist of all the initial requirements and at least two signatures of individuals that have first-hand knowledge the

needs have been met. Having a minimum of two individuals in the acceptance process can provide the checks and balances needed to ensure nothing was missed.

6. Commissioning

That last step of commissioning after testing is how the alternative process ends. This is the final step that includes finalizing all of the ownership documentation, ensuring all the invoices have been paid, and ensuring the ongoing operations can be supported with all of the final deliveries of the process. This includes a survey on the efficacy of the process itself, along with the different component supplies within the process. As the final step, this will include all of the local closeout contract paperwork and will normally identify the start date of the warranty, maintenance and operations phase of the security solution.

D. COMPARISON TO DESIRED CHARACTERISTICS

1. Simple

The RADITC Process could be used by anyone who has basic management skills but will require a detailed support package for each step that includes all of the details to help with the development of artifacts for each step or certified security experts to help at certain times. All of the steps can be modified for each specific problem set or issues, but the steps themselves, and the order they fall in are required to make the use of this method a success.

The alternative analysis activity can be a detailed engineering approach or something as simple as a basic list of all the viable solution with the pros and cons associated with them to resolve an issue within the current environment. How detailed or the format of this effort is not as important as being able to identify technical and nontechnical solutions for each requirement, along with the relative cost as an implementation and operation for each. This should provide all of the stakeholders involved enough information to judge what alternative solution would fit best within the way they operate without requiring a full design and detailed cost estimate for each proposed solution. Solutions should not be biased to a particular technology or distinctive

attributes of a specific vendor. Every problem has at least two viable solutions to choose from, if they are looked at from an objective point of view.

A detailed design is the next step after the selections of the proposed solutions are determined. The design should take into consideration all the interfaces, needs and constraints based on the location in consideration that was discovered in the requirements generation process. The design should also include the adaptation of any regulatory information required and include life safety as a primary consideration. If required, certified personnel to include a registered engineer should endorse the design when any construction activities are required. Stakeholder approval is the final step in the design process.

The implementation step is straightforward and should include the operation and user manuals, along with user training to ensure the system is fully integrated into the operation of the target location.

The next major activity is a key component of the entire process. Testing of the system should be completed to ensure the original requirements have been satisfied. A common practice is to test against the design to see if the design product is installed properly. This requires the assumption that the design fully satisfies the original requirements and any modification and changes made in the implementation had no impact on solving the original security concern.

The alternative process facilitates the capture of the end-users requirements. This ensures any proposed solution is integrated into the current operations. Testing against the end users needs is a separate step within the new process and the solution is not tested against its own design as completed. As in the commercial methodology, there is no requirement to be certified or a trained subject matter expert to use the process, but the more anyone uses any process or methodology, the easier it is to implement. There are no references to a specific location or technology.

The data points are connected and simple to understand with a clear meaning or task. Every step is clear and easy to understand. There is no ambiguity on the order and inputs of each step and there is a clear path between each step. The new process is easy to

use. The process is not tied to or makes any reference to a specific technology or solution type. This meets all of the requirements for the simple characteristic.

2. Repeatable

For a process to be repeatable, it must be technology, solution and location agnostic. This has no steps in the process that requires a specific solution. Location considerations or location specific risk activities are not a component of this process. The analysis of alternatives activity clearly provides for the identification of several alternative solutions. An emphasis should always be on lower cost operational solutions prior to any implementation of any technical solution. A technical solution should always be the consideration of last resort. The alternative process is repeatable because it is both technology and location agnostic.

3. Effective

An effective solution is one that creates a good set of end user requirements and more important test the solution against those requirements. A common practice in the security industry has an expert determining solutions based on individual experience or a limited tool. The solution is then tested to ensure it meets the design requirements of that expert. Two key components of the DoD life cycle acquisition model are the alternative of analysis process and testing against the initial end user requirements. The last of the major activities in the new method will ensure the proposed solution will meet the user's needs. The first major activity in the alternative solution is the development of end user requirements.

In determining if the alternative solution proposed is useful, it must answer yes to the following three questions:

1. Does it clearly define requirements by supporting the identification of the end user needs?

2. Can it facilitate the integration of daily activities to ensure a solution will be utilized?

3. Will it test the solution directly against the identified needs?

The alternative solution developed in this paper will support the identification of the end users needs and test against those needs. Another practice not commonly found within today's modern application of electronic security systems revolves around the solutions integration within the daily activities of its end users.

Too many times a computer, monitor, keypad or some other human interface in placed in an office or on the wall with no integration of that electronic security solution into any regular activity. This electronic system, along with any other item not regularly used, will go unattended and in time may be turned off, if not just ignored completely. This renders all of the cost and effort in designing and implementing a security solution a failure.

Two subprocess steps are found in both the implementation and design phases of the new alternative solution. The design phase has subcomponents titled design system and develops operations and policy interfaces. These are based off of the large federal life cycle model and provide the framework for the integration into the regular operations prior to the implementation phase. The design system subcomponent is self-explanatory. Once a solution is clearly defined and designed, the operational policies for the use of the system and how they interface with the solution should be developed prior to the installation takes place. The identification of issues relating to the existing or proposed policies should be considered prior to this installation in case this activity requires a modification in design. Too many times a solution is developed and installed without the consideration of training, policies and local laws and regulations leaving the system ineffective, if not useable by the end user community.

The implementation phase includes the subprocess of installation and implements the design and verifies integration of the solution within the daily operations. The alternative process can be effective solution.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

> *If I had an hour to solve a problem and my life depended on the solution, I would spend the first 55 minutes determining the proper question to ask, for once I know the proper question, I could solve the problem in than five minutes.* –Albert Einstein

A. SUMMARY

The majority of the processes for the development and validation from requirements to testing of electronic security systems are not effective or easy to use. This assessment made it clear that the commercial option is a viable solution with other considerations added, but the best solution would be the new alternative process developed here. Current electronic security practices start with a site survey, and then go directly into equipment selection and system design. This does not provide for clearly defined end-user requirements or testing a proposed solution against it.

The literature reviewed associated with electronic security systems generally did not agree that specifications are made up of functional and nonfunctional requirements. They usually provided a step that included some set of questions or surveys that are suppose to lead into the development of a requirement. However, there is no clear consensus on what are the end users' needs at each application, how to capture them or even consider them as part of a process to design a security system. A majority of the processes currently found in the literature are highly dependent on the skill of the practitioner to determine solutions with little to no empirical data inputs. None of the process found currently in use have a step that tested or validated that the system met the initial requirements, with no definition of what a requirement should look like or the type of data it should contain. The implementation of this new alternative process will enable those involved in all phases of a system implementation to have a clear and direct understanding of the actual needs. This will improve the overall physical security solutions developed and used by the homeland security community.

Theories and concepts from other applications or problem solving techniques can make an important contribution to the process of developing descriptive end-user

requirements. The identification and addition of that process to the current best practices can enable those involved in all phases of a system implementation to have a clear and direct understanding of the actual needs more effectively. This will improve the overall physical security solutions developed and used by the homeland security community. Requirements define the problem and technical specifications define the solution to the problem (Cellucci, 2008, p. 8). Technology is not the only solution and should never stand-alone. Even when technology, employees and security staff cooperates, security can be weakened without policy and procedures supporting the security measures (Gregory, 1994, p. 10).

B. ADDITIONAL CONSIDERATIONS

In 2006, a terrorist plot was foiled planning to destroy up to ten commercial aircraft traveling from the United Kingdom to North America. The terrorist planned to use liquid explosives for this event and this resulted in a ban on all liquids over a specific size on flights within the United States. According to Kip Hawley (2012), The Transportation Security Administration bans liquids as a policy solution instead of a technology solution because it could be implemented within a day, cost significantly less and functions as good, if not better, than any current technology available. This is a clear example that technology is not the only solution for security related issues.

1. DOTMLPF

The Department of Defense (DoD) has adopted the Doctrine, Organizations Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) problem-solving construct (U.S. Army, 2005, p. 56).

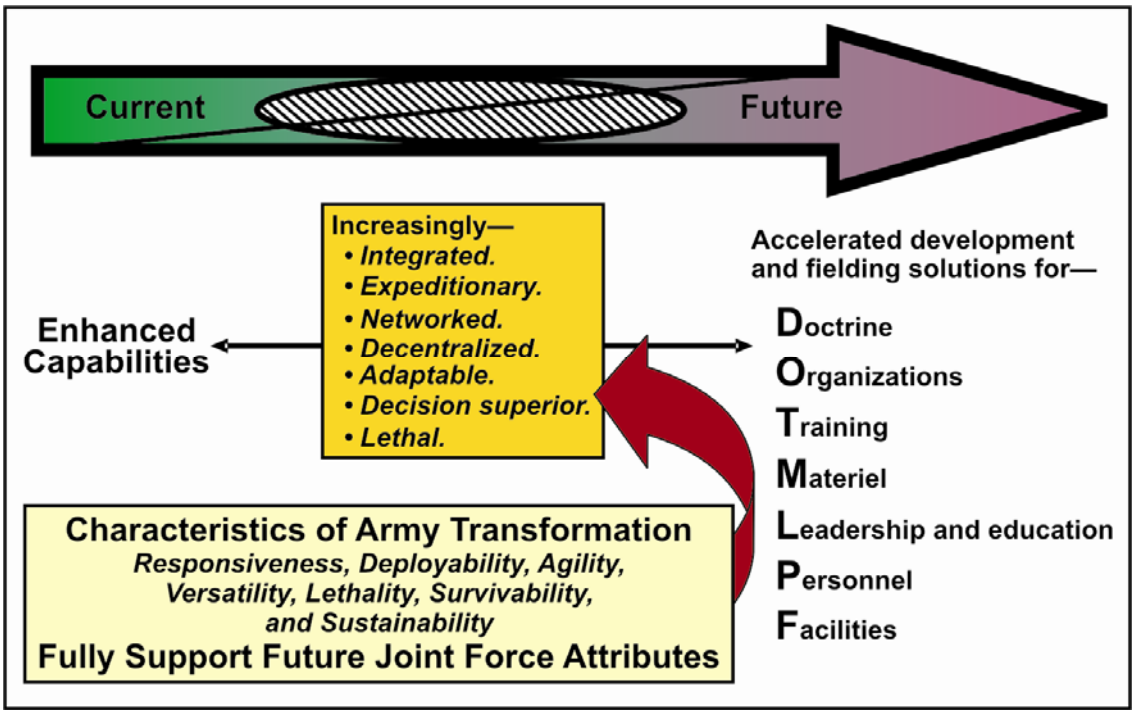

Figure 6. DOTMLF (From FM1 p. 57)

This is used when the DoD is faced with a need that it has not encountered before and requires a solution. In this construct, the first step is Doctrine. In the basic form, this is consider the way things get done on a regular basis. The first look at an alternative solution is based on answering the question can we change the way we do business to solve the problem? The next consideration is organization and then training. Only after these considerations are made does the department consider a material solution. This is an important fact since a material solution is usually the first choice when looking at most security concerns. Leadership change or education, staffing and building are final considerations when looking to solve a problem by the Department of Defense.

C. FURTHER STUDIES

There are a limited number of scientific studies in the field of electronic security. There are a few studies on the effectiveness of video surveillance used in public locations and many studies on the ability of operators that actively monitor video surveillance systems. Many federal and private organizations have done site-specific test to see if an

electronic security system functions as advertised within a specific location or scenario. This research found no formal scientific studies of Electronic Security Systems providing an additional level of security. The RADITC Process is a new process to develop an effective electronic security solution. This new process will need validation with real world applications. Additional studies are needed on the effectiveness of electronic security systems as a whole.

LIST OF REFERENCES

Alrajeh, D., Kramer, J., Russo, A., & Uchitel, S. (2009). Learning operational requirements from goal models. *31st international conference on software engineering, 2009. ICSE 2009.* (p. 265–275). Piscataway, NJ: IEEE.

Argospress. (2012). Performance requirement. Retrieved September 18, 2012, from http://www.argospress.com/Resources/systems-engineering/zperforequir.htm

ASIS. (2012). Brief history of ASIS certifications: A vision to advance security worldwide becomes reality. Retrieved December 4, 2012, from http://www.asisonline.org/certification/brief-history.xml

Biringer, Betty E.: Matalucci, Rudolph V.: O'Connor, Sharon L. (2007). *Security risk assessment and management: A professional practice guide for protecting buildings and infrastructures*. Hoboken, NJ: John Wiley.

Buede, D. M. (1997). Developing originating requirements: Defining the design decisions. *IEEE Transactions on Aerospace and Electronic Systems, 33*(2), 596–609.

Capel, V. (1999). *Security systems and intruder alarms*. Oxford; Boston: Newnes.

Cellucci, T. A. (2008). *Developing operational requirements: A guide to the cost-effective and efficient communication of needs.* Washington, DC: Department of Homeland Security.

Centre for the Protection of National Infrastructure. (2010). *Guide to producing operational requirements for Security Measures.* London, England: Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure. (2012). Physical Security. Retrieved August 12, 2012, from http://www.cpni.gov.uk/advice/Physical-security/

Cook, W. J. (1982). *Security Systems: Considerations, layout, and performance*. Indianapolis, IN: H.W. Sams.

Cornell University. (2012). Legal information institute. Retrieved November 4, 2012, from http://www.law.cornell.edu/uscode/text/10/181

Defense Acquisition University (DAU). (2001). *Systems engineering fundamentals.* Fort Belvoir, VA: Defense Acquisition University.

Defense Acquisition University (DAU). (2008). *Intermediate systems planning, research, development and engineering (SYS202).* Fort Belvoir, VA: Defense Acquisition University.

Defense Acquisition University (DAU). (2009). *Defense acquisition guidebook.* Ft. Belvoir, VA: The Defense Acquisition University (DAU).

DGA Security Systems. (2012). Alarm industry history. Retrieved October 10, 2012, from http://www.dgasecurity.com/about-dga/alarm-industry-history/

Edwards, M. L., Flanzer, M., Terry, M., & Landa, J. (1995). RECAP: A requirements elicitation, capture and analysis process prototype tool for large complex systems. *Engineering of complex computer systems, 1995. held jointly with 5th CSESAW, 3rd IEEE RTAW and 20th IFAC/IFIP WRTP, proceedings., first IEEE international conference on* (pp. 278-281). New York: IEEE Press.

Fennelly, L. J. (2004). *Effective physical security* (3rd ed.). Amsterdam; Boston: Elsevier Butterworth Heinemann.

The Freedonia Group. (2010). *World security equipment: Industry study with forecast for 2014 & 2019*. Cleveland, OH: The Freedonia Group.

The Freedonia Group. (2011). *World security services: Industry study with forecasts for 2014 & 2019*. Cleveland, OH: The Freedonia Group.

Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Boston, MA: Butterworth-Heinemann.

Gerrard, G., Parkins, G., Cunningham, I., Jones, W., Hill, S., & Douglas, S. (2007). *National CCTV strategy.* London, UK: Crown.

Gilbert, R. S., & Chiang, K. S. (1986). Development of a reliable multi-camera multiplexed CCTV system for safeguards surveillance. *Nuclear Materials Management, 15*, 332–338.

Google. (2012). Dow, .dji. Retrieved July 1, 2012, from https://www.google.com/finance?q=NYSE%3Adow+jones+industrial+average

Google. (2012). L-3 communications holdings, inc. (NYSE:LLL). Retrieved July 2012, 2012, from https://www.google.com/finance?client=ob&q=NYSE:LLL

Google. (2012). Lockheed martin corporation (NYSE:LMT). Retrieved July 1, 2012, from https://www.google.com/finance?q=NYSE%3ALMT

Google. (2012). URS corp (NYSE:URS). Retrieved July 1, 2012, from https://www.google.com/finance?q=NYSE%3Aurs

Google.com. (2012). Siemens AG (ADR) (NYSE:SI). Retrieved July 1, 2012, from https://www.google.com/finance?q=NYSE%3Asi

Gordon, K. A., & Wyss, G., D. (2005). *Comparison of two methods to quantify cyber and physical security effectiveness*. Albuquerque, NM: Sandia National Laboratories.

Gregory, W. L. (1994). Halt! is your security system secure? *HR Focus, 71*(2), 9–10.

Hall, A. (1998). What does industry need from formal specification techniques? *Industrial strength formal specification techniques, 1998. proceedings. 2nd IEEE workshop on* (pp. 2-7). New York: IEEE Press.

Halligan, R. (2012). *What is the significance of different types of requirements such as states and modes, functional, performance, external interface, environmental, resource, physical, other qualities and design?*. Victoria, Australia: Project Performance International. Retrieved from http://www.ppi-int.com/systems-engineering/types-of-requirements.php

Hawley, K., & Means, N. (2012). *Permanent emergency: Inside the TSA and the fight for the future of American security* Palgrave Macmillan.

Headquarters United States Marine Corps. (2000). *Marine Corps physical security manual.* (No. MCO P5530.14). Navy Annex, Washington DC: Department of the Navy.

Hoffman, G. (1989). The first line of defense. *Security Management,* 73–75.

Honey, G. (1998). *Electronic protection and security systems*. Oxford; Boston: Newnes.

Honey, G. (1999). *Newnes electronic security systems pocket book.* Oxford; Boston: Newnes.

Humberside Police. (2012). Centre for the protection of the national infrastructure (CPNI). Retrieved October 18, 2012, from http://www.humberside.police.uk/what-we-do/project-argus---protecting-against-terrorist-attack/centre-for-the-protection-of-the-national-infrastructure-cpni

Kaiya, H., & Ohnishi, A. (2011). Quality requirements analysis using requirements frames. In IEEE Reliability Society (Ed.), *11th international conference on quality software (QSIC) : Madrid, Spain, 13-14 July 2011* (pp. 198-207). Piscataway, NJ: IEEE.

Keating, M. (2010). Government security spending. *GovPro Media*, February 24, 2010.

Letourneau, J. P. (2009). *Incorporating multi-criteria optimization and uncertainty analysis in the model-based systems engineering of an autonomous surface craft* (Master's thesis). Naval Postgraduate School.

Lormans, M. (2007). Monitoring requirements evolution using views. *CSMR 2007: 11th European conference on software maintenance and reengineering: Proceedings: 21-23 march, 2007.* (pp. 349–352). Los Alamitos, CA: IEEE Computer Society.

Malan, R., & Bredemeyer, D. (2001). *Defining non-functional requirements.* Bloomington, IN: Bredemeyer Consulting.

Malan, R., & Bredemeyer, D. (2012). Functional requirements and use cases. Retrieved January 20, 2012, from http://www.bredemeyer.com/use_cases.htm

Mitre. (2012). Systems engineering life-cycle blocks. Retrieved November 7, 2012, from http://www.mitre.org/work/systems_engineering/guide/se_lifecycle_building_blocks/concept_development/operational_requirements.html

Norman, T. L. (2007). *Integrated security systems design concepts, specifications, and implementation*. Amsterdam; Boston: Elsevier Butterworth-Heinemann.

Ohlhausen Research, I. (1993). *False alarm perspectives: A solution-oriented resource.* Alexandria, VA: International Association of Chiefs of Police.

Oxford University. (2012). Oxford English dictionary. Retrieved August 15, 2012, from http://www.oed.com

Pearson, R. L. (2007). *Electronic security systems a manager's guide to evaluating and selecting system solutions*. Amsterdam; Boston: Butterworth-Heinemann.

Pelco. (2012). Pelco global training institute. Retrieved December 4, 2012, from http://www.pelco.com/sites/global/en/services/pelco-global-trianing-institute/pgti.page

Pitman, P. M., & Wollman, L. F. (2009). *Research methods part II: Policy options analysis* (https://www.chds.us/coursefiles/NS4081/lectures/methods_policy_options_analysis_v02/player.html ed.) Center For Homeland Defense and Security.

Project Performance International. (2011). Types of requirements. Retrieved December 12, 2011, from http://www.ppi-int.com/systems-engineering/types-of-requirements.php

Prokop, J. (2012). The office of security capabilities, advanced surveillance program. Arlington, Va.

Raja, U. A. (2009). Empirical studies of requirements validation techniques. *2nd international conference on computer, control and communication, 2009: Karachi, Pakistan, February 17-18, 2009.* (pp. 1–9). Piscataway, NJ: IEEE.

Sampson, R. (2011). *False burglar alarms: Second edition.* Washington, DC: Center for Problem-Oriented Policing, Inc.

Sandia National Laboratories. (2012). Physical Security. Retrieved July 1, 2012, from http://www.sandia.gov/mission/homeland/programs/hdfp/hdfp-physical.html

Seungmug, L. (2008). *The impact of home burglar alarm systems on residential burglaries.* Rutgers, NJ: The School of Criminal Justice, Rutgers University.

Snyder, N. H., & Caswell, J. L. (1989). An overview of physical security devices. *Industrial Management, 31*(4), 25–29.

Spaight, W. H. T. (2000). Operational requirements for security measures. *34th annual 2000 international carnahan conference on security technology, 2000. proceedings: IEEE: October 23-25, 2000, Ottawa, Ontario, Canada.* (pp. 64-70). Piscataway, NJ: IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber =891169&tag=1

SPAWAR Systems Center. (2006). CCTV technology handbook.

Szuba, T. (1998). *Safeguarding your technology: Practical guidelines for electronic education information security.* Washington, DC: National Center for Education Statistics (ED), National Postsecondary Education Cooperative; National Forum on Education Statistics.

Twain, M. (1922). *The mysterious stranger and other stories* (1st ed.). New York: Harper & Bros.

United Kingdom Home Office. (2012). Security industry authority. Retrieved August/20, 2012, from http://www.sia.homeoffice.gov.uk/Pages/about-us.aspx

U.S. Army. (2005). *fm1*. Washington, DC: Department of the Army.

U.S. Army Military Police School. (2001). *FM 3-19.30 physical security*. Fort Leonard Wood, MO: U.S. Army.

U.S. Department of Homeland Security (DHS). (2012). About SAVER. Retrieved January 21, 2012, from https://www.rkb.us/SAVER/SaverAbout.cfm?action =Background

Wasson, C. S. (2005). *System analysis, design, and development: Concepts, principles, and practices*. Hoboken, NJ: Wiley-Interscience.

Whittle, T. J. (1987). Security by design. *Security Management*, 57–60.

Wiegers, K. (1999). Writing quality requirements. *Software Development, 7*(5), 44-48. Retrieved from http://search.proquest.com/docview/222133187?accountid=12702

Williams, J. D. (1997). *Physical protection systems design and evaluation.* (). Albuquerque, NM: Sandia National Labs. Retrieved from http://www.osti.gov/bridge/purl.cover.jsp?purl=/456312-ovreos/webviewable/

Zoufal, D. (2008). *Someone to watch over me? Privacy and governance strategies for CCTV and emerging surveillance technologies* (Master's thesis). Naval Postgraduate School).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California